IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1. (Previously Presented) A method for authenticating at least one of a media and data stored on said media, in order to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on said media, wherein said data stored on said media is modulated via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating at least one of said media and said data, said method comprising the steps of:

(a) reading the data from said media;

(b) detecting the modulation of the at least one modified modulation rule associated with the data;

(c) deriving an embedded authentication key or component thereof responsive to said detecting step (b);

(d) comparing the embedded authentication key or component thereof, to at least one authentication key or component thereof;

(e) authenticating the at least one of said media and said data responsive to said comparing step (d); and

(f) outputting said data as at least one of audio, video, audio data, video data and digital data substantially free of the modulation of the at least one modified modulation rule.

Claim 2. (original) A method according to claim 1, wherein said deriving step (c) derives the embedded authentication key or component thereof as a combination of on-off binary codes representing ones and zeros to represent a predetermined symbol sequence.

Claim 3. (original) A method according to claim 1, wherein said outputting step (f) further includes the step of converting said data into a stereo analog signal without transferring, in the data, the modulation of the at least one modulation rule used to derive the embedded authentication key or component thereof.

Claim 4. (original) A method according to claim 1, and further including the step of:

(g) locating at least one modified modulation rule on at least one of a per track basis and interval basis throughout said media such that said authentication step (e) is performed for at least one of each track to be played, throughout playback and throughout recording.

Claim 5. (original) A method according to claim 1, wherein said authenticating step (e) further includes a step of authenticating using a different authentication key or component thereof for each disc track.

Claim 6. (original) A method according to claim 1, said method comprises the step of authenticating the at least one of the data and the media via at least two different authentication keys, each of which successively must be authenticated before said data is finally output via said outputting step (f).

Claim 7. (original) A method according to claim 1, wherein said method authenticates the at least one of the media and the data over a plurality of interconnected computer networks comprising at least one of a local network, global network and the Internet.

Claim 8. (original) A method according to claim 1, wherein said authenticating step (c) further includes a step of using at least three different sources for compiling compound authentication keys.

Claim 9. (original) A method according to claim 1 wherein said deriving step (c) further comprises the step of at least one of decoding and decrypting the embedded authentication key or component thereof for subsequent authentication.

Claim 10. (original) A method according to claim 1 wherein said comparing step (d) further comprises the step of comparing the at least one modified modulation rule comprising the at least one authentication key or component thereof, to at least one lookup table of valid modified modulation rule output values comprising the at least one authentication key or component thereof.

Claim 11. (Previously Presented) In a method for authenticating at least one of a media and data stored on said media, in order to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on said media, a data disc comprising media containing at least one modified modulation rule comprising at least one authentication key or component thereof for authenticating at least one of said media and said data, wherein said at least one of said media and said data may be outputted in at least one of an analog and audio form substantially error free and free of said at least one modified modulation rule by at least one of an error removal process and said at least one authentication key or component thereof, thereby allowing a user to experience said media without experiencing said modulation rules removed therefrom via said error removal process.

Claim 12. (Previously Presented) In a method for authenticating at least one of a media and data stored on said media, in order to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on said media, wherein said data stored on said media is modulated via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating at least one of said media and said data, a data player comprising a data processor performing the steps of:

(a) reading the data from said media;

(b) detecting the modulation of the at least one modified modulation rule associated with the data;

(c) deriving an embedded authentication key or component thereof responsive to said detecting step (b);

(d) comparing the embedded authentication key or component thereof, to at least one authentication key or component thereof;

(e) authenticating at least one of said media and said data responsive to said comparing step (d); and

(f) outputting said data as at least one of audio, video, audio data, video data and digital data substantially free of the modulation of the at least one modified modulation rule.

Claim 13. (original) In a method for authenticating at least one of a media and data to be stored on said media, in order to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on said media, a data message comprising modulation via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating said data message, and wherein the modified modulation rule cannot be readily altered, obscured nor removed from said data message without simultaneously degrading or impairing a quality of an audible component of said data message, and wherein the data message is transmitted substantially free of the modified modulation rule thereby preventing a destination processor from reading and subsequently authenticating said data message.

Claim 14. (Previously Presented) A system for authenticating at least one of a media and data stored on said media, in order to prevent at least one of piracy, unauthorized access and

unauthorized copying of the data stored on said media, wherein said data stored on said media is modulated via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating at least one of said media and said data, wherein said at least one of said media and said data may be outputted in an analog and/or audio form substantially error free and free of said at least one modified modulation rule by at least one of an error removal process and said at least one authentication key or component thereof, said system including a data player containing a data processor comprising lookup table means for authenticating said at least one of said media and said data and for intentionally breaking standard modulation rules by which bit patterns are recorded as one or more symbol sequences on a data media, said lookup table means connected to a focus servo, tracking servo, laser, lens and mirror, together comprising a portion of a disc reader housed in a data player device.

Claim 15. (Previously Presented) A system for authenticating at least one of a media and data stored on said media, in order to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on said media, wherein said data stored on said media is modulated via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating at least one of said media and said data, wherein said at least one of said media and said data may be outputted in an analog and/or audio form substantially error free and free of said at least one modified modulation rule by at least one of an error removal process and said at least one authentication key or component thereof,

said system including a data player containing a data processor comprising a lookup table used by said data processor in intentionally modifying at least one modulation rule by which at

least one bit indicative of said modifying is generated as at least one symbol used by said system to authenticate said at least one of said media and said data stored on said media.

Claim 16. (Previously Presented) A system for authenticating at least one of a media and data stored on said media, in order to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on said media, wherein said data stored on said media is modulated via at least one modified modulation rule to generate at least one authentication key or component thereof for authenticating at least one of said media and said data, said system comprising:

means for reading the data from said media;

means for detecting the modulation of the at least one modified modulation rule associated with the data;

means for deriving an embedded authentication key or component thereof responsive to said means for detecting;

means for comparing the embedded authentication key or component thereof, to at least one authentication key or component thereof;

means for authenticating the at least one of said media and said data responsive to said means for comparing; and

means for outputting said data as at least one of audio, video, audio data, video data and digital data substantially free of the modulation of the at least one modified modulation rule.

Claim 17. (Previously Presented) The system of claim 16, wherein said means for deriving includes means for deriving the embedded authentication key or component thereof as a combination of on-off binary codes representing ones and zeros to represent a predetermined symbol sequence.

Claim 18. (Previously Presented) The system of claim 16, wherein said means for outputting includes means for converting said data into a stereo analog signal without transferring, in the data, the modulation of the at least one modulation rule used to derive the embedded authentication key or component thereof.

Claim 19. (Previously Presented) The system of claim 16, further comprising means for locating at least one modified modulation rule on at least one of a per track basis and interval basis throughout said media such that said means for authenticating authenticates for at least one of each track to be played throughout playback and throughout recording.

Claim 20. (Previously Presented) The system of claim 16, wherein said means for authenticating further includes means for authenticating using a different authentication key or component thereof for each disc track.

Claim 21. (Previously Presented) The system of claim 16, wherein said means for authenticating further includes means for authenticating using at least two different authentication key, each of which must be successively authenticated before said data is output.

Claim 22. (Previously Presented) The system of claim 16, wherein said means for authenticating further includes means for authenticating using at least three different sources for compiling compound authentication keys.

Claim 23. (Previously Presented) The system of claim 16, wherein said means for authenticating further includes at least one of means for decoding or decrypting the embedded authentication key or component thereof for subsequent authentication.

Claim 24. (Previously Presented) The system of claim 16, wherein said means for comparing further includes means for comparing the at least one modified modulation rule to at least one lookup table of valid modified modulation rule output values comprising the at least one authentication key or component thereof.

Claim 25. (Previously Presented) The data disc of claim 11, wherein said at least one modified modulation rule is located on at least one of a per track basis and interval basis throughout said media such that authenticating is performed for at least one of each track to be played throughout playback and throughout recording.

Claim 26. (Previously Presented) The data disc of claim 11, wherein authentication occurs using a different authentication key or component thereof for each disc track.

Claim 27. (Previously Presented) The data disc of claim 11, wherein authentication occurs using at least two different authentication key, each of which must be successively authenticated before said data is output.

Claim 28. (Previously Presented) The data disc of claim 11, wherein authentication occurs using at least three different sources for compiling compound authentication keys.

Claim 29. (Previously Presented) The data disc of claim 11, wherein authentication occurs via decoding or decrypting the embedded authentication key or component thereof for subsequent authentication.

Claim 30. (Previously Presented) The data processor of claim 12, wherein said step of deriving includes deriving the embedded authentication key or component thereof as a combination of on-off binary codes representing ones and zeros to represent a predetermined symbol sequence.

Claim 31. (Previously Presented) The data processor of claim 12, wherein said step of outputting includes converting said data into a stereo analog signal without transferring, in the data, the modulation of the at least one modulation rule used to derive the embedded authentication key or component thereof.

Claim 32. (Previously Presented) The data processor of claim 12, wherein said data processor further performs the step of locating at least one modified modulation rule on at least one of a per

track basis and interval basis throughout said media such that said authenticating authenticates for at least one of each track to be played throughout playback and throughout recording.

Claim 33. (Previously Presented) The data processor of claim 12, wherein said step of authenticating further includes authenticating using a different authentication key or component thereof for each disc track.

Claim 34. (Previously Presented) The data processor of claim 12, wherein said step of authenticating further includes authenticating using at least two different authentication key, each of which must be successively authenticated before said data is output.

Claim 35. (Previously Presented) The data processor of claim 12, wherein said step of authenticating further includes authenticating using at least three different sources for compiling compound authentication keys.

Claim 36. (Previously Presented) The data processor of claim 12, wherein said step of authenticating further includes at least one of decoding or decrypting the embedded authentication key or component thereof for subsequent authentication.

Claim 37. (Previously Presented) The data processor of claim 12, wherein said step of comparing further includes comparing the at least one modified modulation rule to at least one lookup table

of valid modified modulation rule output values comprising the at least one authentication key or component thereof.

Claim 38. (Previously Presented) The data message of claim 13, wherein said at least one modified modulation rule is located on at least one of a per track basis and interval basis throughout said media such that authenticating is performed for at least one of each track to be played throughout playback and throughout recording.

Claim 39. (Previously Presented) The data message of claim 13, wherein authentication occurs using a different authentication key or component thereof for each disc track.

Claim 40. (Previously Presented) The data message of claim 13, wherein authentication occurs using at least two different authentication key, each of which must be successively authenticated before said data is output.

Claim 41. (Previously Presented) The data message of claim 13, wherein authentication occurs using at least three different sources for compiling compound authentication keys.

Claim 42. (Previously Presented) The data message of claim 13, wherein authentication occurs via decoding or decrypting the embedded authentication key or component thereof for subsequent authentication.

Claim 43. (Previously Presented) The system of claim 14, wherein said at least one modified modulation rule is located on at least one of a per track basis and interval basis throughout said media such that authenticating is performed for at least one of each track to be played throughout playback and throughout recording.

Claim 44. (Previously Presented) The system of claim 14, wherein authentication occurs using a different authentication key or component thereof for each disc track.

Claim 45. (Previously Presented) The system of claim 14, wherein authentication occurs using at least two different authentication key, each of which must be successively authenticated before said data is output.

Claim 46. (Previously Presented) The system of claim 14, wherein authentication occurs using at least three different sources for compiling compound authentication keys.

Claim 47. (Previously Presented) The system of claim 14, wherein authentication occurs via decoding or decrypting the embedded authentication key or component thereof for subsequent authentication.

Claim 48. (Previously Presented) The system of claim 15, wherein said at least one modified modulation rule is located on at least one of a per track basis and interval basis throughout said

media such that authenticating is performed for at least one of each track to be played throughout playback and throughout recording.

Claim 49. (Previously Presented) The system of claim 15, wherein authentication occurs using a different authentication key or component thereof for each disc track.

Claim 50. (Previously Presented) The system of claim 15, wherein authentication occurs using at least two different authentication key, each of which must be successively authenticated before said data is output.

Claim 51. (Previously Presented) The system of claim 15, wherein authentication occurs using at least three different sources for compiling compound authentication keys.

Claim 52. (Previously Presented) The system of claim 15, wherein authentication occurs via decoding or decrypting the embedded authentication key or component thereof for subsequent authentication.